The National Science Foundation
Office of Polar Programs
United States Antarctic Program

Information Resource Management Directive 5000.15
USAP Information Resource Configuration Management

Organizational Function	Information Resource Management	Policy Number	5000.15
		Issue Date	1 August 2004
Policy Category	Information Security Policies and Procedures	Effective Date	1 August 2004
		Review On	1 August 2006
Subject	Information Resource Configuration Management	Authorized By	Director, OPP
Office of Primary Responsibility	National Science Foundation Office of Polar Programs Polar Research Support Section	Responsible Official	Mr. Patrick D. Smith Technology Development Manager
Address	Suite 755 4201 Wilson Blvd Arlington, VA 22230	Phone	703.292.8032
		Fax	703.292.9080
		Web	www.nsf.gov/od/opp
Distribution	USAP-Wide	Status	Final Policy
Online Publication	www.polar.org/infosec/index.htm		

1. PURPOSE

This policy establishes the guidelines for managing the configurations of and the changes made to information resources within the National Science Foundation (NSF) Office of Polar Programs (OPP), United States Antarctic Program (USAP). Additions, deletions, and modifications to operational information resources must be accomplished according to an enterprise process for configuration and change management. This policy also establishes the position of the USAP Information Resource Configuration Manager to serve as the central configuration management authority for all USAP information resources.

2. BACKGROUND

Federal information technology regulations require administrators and users of USAP information resources to follow an established process for changing any component or sub-component of the USAP information infrastructure. Establishing and maintaining a strong configuration and change management program protects information resources

from unauthorized modifications that could undermine the science and operations activities of the USAP.

3. GUIDING PRINCIPLES

- Configuration management will enhance a system's capability to meet USAP mission needs.
- Configuration changes will balance the need to maintain system security with the need to meet changes in the operational mission.
- Configuration Management will increase the occurrence of planned proactive behavior by reducing the need for unscheduled reactionary behavior.
- Configuration Management will facilitate the orderly management of remote information resources operated by transient personnel

4. POLICY

The NSF Office of Polar Programs will assign Configuration Management responsibilities to a single USAP participant organization. That organization will establish a process to standardize and manage the configuration of and changes to all USAP information resources. Once established, all USAP information resources will conform to the USAP Configuration Management process.

4.1 Operational Definitions

4.1.1 Audit

The independent examination of a component or system to assess compliance with standards, specifications, contractual agreements or other criteria.

4.1.2 Baseline

The specification or product, which has been reviewed and agreed upon, and thereafter serves as a basis for further development. After being established, the baseline can only be changed through formal configuration control procedures.

4.1.3 Baseline Environment

The fundamental operating environment in which a resource will be first initialized and evaluated against its requirements. The baseline environment sets the foundation for system evaluation, and identifies the basic operating conditions as a reference point for future system improvements. The baseline environment includes the physical installation locations for the integration, test, demonstration and operational environments.

4.1.4 Component

A component is one of the parts that make up a system. A component may be hardware, software, or documentation, and may be composed of other components. A component is an element that can be changed. The terms module, component, and unit may be used

interchangeably or defined to be sub elements of one another in different ways depending on the context.

4.1.5 Configuration

The arrangement of a system or component as defined by the number, nature, or interconnections of its constituent parts. For CM, the functional and physical characteristics of hardware, software, or documentation as set forth in writing or achieved in a system.

4.1.6 Configuration Baseline

A document or set of documents, formally designated and fixed at a specific time and constituting the approved configuration identification of a configuration item. Documents usually refer to specifications and drawings for hardware, firmware, and software and include listings, flowcharts, and decision trees. Concepts of operations and operational procedures for a configuration item may also be included in the configuration baseline.

4.1.7 Configuration Control

One element of configuration management consisting of the evaluation, coordination, approval, and implementation of changes to components after having formally established a configuration identification (baseline).

4.1.8 Configuration Control Board

The group responsible for evaluating and approving proposed changes to configuration items or components. The Configuration Control Board is the Configuration Management Authority for USAP information resources.

4.1.9 Configuration Identification

Selection of configuration items and maintenance of the documents that identify and define the baseline of a configuration item or the overall system. This includes the determination of the types of configuration documentation for each configuration item, the issuance of unique identifiers affixed to each configuration item, and the technical documentation that defines the configuration item's configuration.

4.1.10 Configuration Item

Aggregation of hardware, software or both which has been designated for configuration management and processed as a single entity through the configuration management System.

4.1.11 Configuration Management

A discipline applying technical and administrative directives and surveillance to identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and to verify compliance with specified requirements.

4.1.12 Consistency

The degree of uniformity, standardization, and freedom from contradiction among the documents or parts of a system or component.

4.1.13 Emergency Change

An Emergency Change is a change that must be made in response to a situation involving potential injury or loss of life, or an ongoing or pending disaster or contingency.

4.1.14 Functional Configuration Audit

An audit to verify that a configuration development item is completed satisfactorily. The audit verifies and documents that the item has achieved the functional and performance characteristics specified in requirements, and that all operational or support publications have been approved and posted for use.

4.1.15 Physical Configuration Audit

An Audit to verify that a configuration item, as built, conforms to the requirements that defined the effort.

4.1.16 Product Configuration Identification

The approved, or conditionally approved, technical documentation defining a configuration item during the production, operation, maintenance, and logistic support phases of its life cycle. It prescribes all necessary physical or form, fit, and function characteristics of a configuration item, the selected functional characteristics designated for production and acceptance testing, and the production acceptance tests.

4.1.17 Routine Change

A Routine Change is a change that is made as part of normal system maintenance, upgrades or enhancements in response to an identified need.

4.1.18 System

A collection of components organized for a specific function or set of functions.

4.1.19 System Life Cycle

The time frame that encompasses a system's existence, from concept through design to operation and upgrades, until retired or replaced. Different phases managed during this time include definition, design, development, test, demonstration, operation, maintenance, and retirement.

4.1.20 Traceability

The degree to which a relationship can be established between two or more products of the development process, especially products having a predecessor-successor or master-subordinate relationship to one another; for example, the degree to which the requirements and design of a given software component match.

4.1.21 Urgent Change

An Urgent Change is a change that must be made in a timely manner, in response to a situation involving the potential for significant impact to the NSF mission, potential for a known security vulnerability to be exploited, or as identified by NSF OPP.

4.2 Configuration Management Process

4.2.1 Configuration Management Program

The NSF OPP will establish a configuration management program for USAP information resources and designate a single USAP participant organization to serve as the USAP Information Resource Configuration Manager (IRCM). The IRCM will function as the central configuration management authority for all USAP information resources. The Configuration Management Program will include provisions for Change Management of USAP information resources.

4.2.2 Purpose of Configuration Management

The fundamental purpose of Configuration Management is to establish and maintain integrity and control of all project deliverables, throughout their life cycle to system retirement or replacement. Maintaining control of the configuration of an information resource enhances the confidentiality, integrity and availability of the resource and the information it processes. Applying the Configuration Management process improves system performance and extends system serviceability, while minimizing service interruptions during project evolution or sustaining operations. By intent, the Configuration Management Process applies to all aspects of system or service development, implementation, and operation, to include performance requirements, functional attributes, physical attributes, design information, operation information and procedures, and security characteristics.

4.2.3 Change Management Process

Change Management applies the concepts of configuration management in a process to track approved changes to information resources. The Change Management process has five basic steps:

- **Step 1, Identification:** This step involves the determination that a change is required to meet an existing operations need, or to respond to a new operations requirement. It includes a description of the needed change including the mission drivers, identification of the affected resources, and a summary of potential solutions. Potential changes should be categorized as Emergency, Urgent, or Routine, depending on the nature of the change.
- **Step 2, Analysis:** This step is a technical evaluation and risk assessment of the change and its effects on the information resource, other connected resources, the enterprise network, and other mission considerations. The outcome of the evaluation is a recommended course of action to be approved and implemented, and an implementation plan that includes a backout strategy should the change prove to be harmful, or ineffective.

- **Step 3, Approval:** This step is the management review and approval of the recommended technical change. It is normally accomplished using a review board, with identified provisions for approval of emergency or urgent changes.
- **Step 4, Implementation:** This step is the implementation of the approved change, at an appropriate time to minimize the impact on mission activities and enterprise operations. Implementation of routine changes will normally occur during scheduled maintenance periods. Implementation of emergency and urgent changes will occur as determined by the approving review board. This step includes a process to notify enterprise users of the pending change, and the expected effects on service during and after the change. This step includes the provision for site discretion with respect to the implementation of emergency and urgent changes in support of site science and operations activities.
- **Step 5, Change Close out:** This step is the after-action report and evaluation of the change as implemented. It confirms to all interested parties that the change has occurred, and has been documented. It identifies the results of the change, and highlights deviations from the planned change that may have resulted from implementation. The after-action report may require further action by one or more enterprise elements as a result of the change.

5. APPLICABILITY AND COMPLIANCE

This policy applies to all information resources, systems, and technology and to all users of these resources, systems and technology within the USAP operating environment or connected to the USAP information infrastructure. Compliance with this policy is as indicated in USAP Information Security Policy 5000.1, *The USAP Information Security Program*.

6. RESPONSIBILITIES

In addition to the responsibilities identified in USAP Information Resource Management Directive 5000.1, The USAP Information Security Program, the following officials have specific responsibilities related to Information Security and Organization.

6.1 NSF Polar Research Support Technology Manager

The NSF Polar Research Support Technology Manager designates the USAP Information System Configuration Manager.

6.2 USAP Information Resource Configuration Manager (IRCM)

The USAP Information Resource Configuration Manager (IRCM) establishes the processes and procedures needed to implement appropriate levels of configuration management for USAP information resources. The USAP Information Resource Configuration Manager establishes and chairs the Configuration Control Board as the configuration management authority for all USAP information resources.

6.3 USAP Information Security Manager

The USAP Information Security Manager ensures configuration management requirements are addressed by USAP information resources, in particular those resources involved in the security of the USAP information infrastructure.

6.4 USAP Information System Managers and Administrators

The USAP Information System Configuration Manager establishes the processes and procedures needed to implement appropriate levels of configuration management for USAP information resources.

7. PROGRAM IMPLEMENTATION

7.1 Establishment

The USAP Information System Configuration Manager will establish the process, standards, and procedures for information resource Configuration Management and organize appropriate staff to execute its functions. Security of information resources will be integrated into the configuration of USAP major applications and general support systems, and in the processes established to manage the configuration of these resources.

7.2 Scope

The USAP Configuration Management process will apply uniformly to all USAP information systems on a continuous basis.

7.3 USAP Configuration Control Board

The USAP Configuration Management process will include the establishment of a central Configuration Control Board to serve as the central configuration management authority for all USAP information resources.

7.4 Policy Review

The USAP Information Resource Configuration Manager and the USAP Information Security Manager will review this policy in conjunction with major changes to the information infrastructure, as part of the USAP's participation in agency security audits, after each breach in system security, or every two years. The IRCM and ISM will submit policy changes and new policies for review and approval by NSF OPP.

8. AUTHORITY

Publication of this policy is in conformance with the authority of the National Science Foundation Act of 1950, as amended and extended, the Federal Information Security Management Act of 2002 and NSF Manual 7, The NSF Information Security Handbook.

KARL A. ERB

Director